PROFESSIONAL SERVICES
RAPID RESPONSE RETAINER
BASIC LEVEL OF SERVICE
STATEMENT OF WORK
TO VERIZON PROFESSIONAL SERVICES SERVICE ATTACHMENT

This Rapid Response Retainer SOW is entered pursuant to the service order form ("SOF") between the entities identified as, respectively, "Verizon" and "Customer" in the SOF executed between Verizon and Customer. Additionally, this SOW is made pursuant to the Master Terms as well as the Professional Service specific terms (the "PSA") each as provided in the SOF. Together with any other terms set forth in this SOW, the SOF, the Master Terms, and PSA are hereinafter collectively referred to as the "Agreement". All capitalized terms used but not expressly defined in this SOW have the meanings given such terms in the Agreement.

1. **Description of the Project.** This SOW defines the professional services and Deliverables that Verizon will provide to Customer under the terms of the Agreement and forms the basis for the pricing in the Rates and Charges Section of the SOF. Verizon will perform a Project, as defined below, at the Customer Sites identified in engagement letters entered into from time to time (the "Engagement Letters") pursuant to the Engagement Letter process set forth below. The Service Commitment and Service Activation Date are shown in the SOF. For the purposes of this SOW, the "Contract Year" means each consecutive twelve (12) month period during the Service Commitment and commencing on the Service Activation Date or its annual anniversary. This SOW, the related SOF, Agreement, and Engagement Letters constitute the entire agreement between the Parties with respect to the Professional Services and any Project and supersede all other prior or contemporaneous representations, understandings or agreements. Except as otherwise expressly stated herein, no amendment to this SOW, SOF, or Engagement Letter is valid unless in writing and signed by both Parties. The Project is limited to the services, Deliverables, documentation and conditions stated herein and in the Agreement.

1.1 **Professional Services.** Verizon will provide Customer with the Rapid Response Retainer Professional Services at the Basic level of service, which may be referred to generally hereafter as "Professional Services" or, for a specific engagement, as a "Project".

1.2 **Scope of Work.** This SOW describes the following Professional Services and procedures related to Customer's preparation for, response to, and management of cyber security incidents. Certain activities will require security consulting support hours ("Hours") and must be requested by Customer using the Engagement Letter process, each as described below.

- Security Consulting Support;
- Onboarding;
- Project Initiation Process (Engagement Letters);
- Cyber Incident Capability Assessments (each, an "Assessment");
- Hotline Access;
- Investigative Liaison;
- Investigative Team Phone Support;
- Emergency Services;
- Malcode Analysis;
- Verizon RISK Intelligence;
- Project Management; and
- Service Level Agreement ("SLA") Terms.

1.2.1 **Security Consulting Support.**

1.2.1.1 **Base Service.** With Rapid Response Retainer base services only, Customer may request any of the Professional Services as described in this SOW, or as described at the following link (the

"Professional Services Terms Link"), with the number of security consulting support Hours shown herein, or on an Engagement Letter, as applicable. Professional Service Hours shall be provided at the hourly rates shown in the SOF.

- Professional Services Terms Link for U.S. Services:

http://www.verizonenterprise.com/external/service_guide/reg/cp_ps_plus_toc.htm

- Professional Services Terms Link for non-U.S. Services:

http://www.verizonenterprise.com/external/service_guide/reg/ps-plus-toc-2018OCT10.htm

1.2.1.2 **Standard Service.** The Rapid Response Retainer standard service includes one hundred (100) Hours of security consulting support to be used within each Contract Year. Security consulting support Hours may be used by Customer towards any of the Professional Services which require security consulting support Hours as described in this SOW or as described at the Professional Services Terms Link. In the event Customer uses all of the Hours within a Contract Year, Customer can request additional Professional Services at the hourly rate shown in the SOF. Additional consulting support hours are requested via an Engagement Letter. Any Hours that have not been used by Customer by the end of any Contract Year will be deemed forfeited by Customer and Verizon has no further obligation with respect to such Hours and no refund, credit or other form of reimbursement will be due by Verizon to Customer.

1.2.2 **Onboarding.** (Requires 0 Hours)

1.2.2.1 Within ten (10) days of the commencement of a Contract Year, Verizon will send an email to Customer's point of contact ("POC") requesting a date and time for an onboarding discussion ("Onboarding"). Onboarding will take place either in person, or via a conference call between Customer and Verizon.

1.2.2.2 During the initial Onboarding session, Verizon will: i) collect Customer contact information, ii) collect the list of countries where Customer may need Professional Services (as provided in the Project Delivery Countries section below) (the "Country List") to be documented in a Country List Schedule; and iii) collect any information required from Customer for registration into the Professional Services. Further, Verizon will review the Professional Service components and the Engagement Letter process for requesting Professional Services for a Project and provide Customer with the name of the Verizon designated investigative liaison, each as further described below. Verizon will provide details related to escalation processes and access to the Verizon portal for uploading Customer files as required.

1.2.2.3 During each Onboarding session, Customer will select one cyber incident capability Assessment from the four available Assessment options and provide its requested schedule for delivery of the Assessment. Verizon and Customer will work together to determine a time for the Assessment that is reasonable for both Parties. Following Onboarding, Verizon will forward the Customer an Engagement Letter for Customer's execution containing the name of the Assessment selected and mutually agreed upon schedule. Additionally, once the Onboarding process is complete, Customer will be able to order Professional Services in addition to the Assessment via the Project initiation process as described below.

1.2.3 **Project Initiation Process (Engagement Letters).**

1.2.3.1 After the Onboarding process is complete, when Customer wishes to request a Professional Service, Customer will contact the Liaison or call the Hotline and initiate the Professional Service via an Engagement Letter as specified herein.

1.2.3.2 The scope of each Engagement Letter will be agreed upon on a case-by-case basis. The Project initiation process takes an average three (3) hours during which Verizon will define and Customer

will agree upon the Project objectives, scope of work, Customer Sites, number of hours to complete and expected Deliverables.

1.2.3.3 When Customer orders a Project, Verizon will provide a written Engagement Letter that describes the Project requested, methodologies to be used in performance of the requested Project, and the number of Hours required to complete the requested Project. Additional or changed Project Hours will require an amended Engagement Letter.

1.2.3.4 All Engagement Letters will be in writing and follow the format of the template shown at the Professional Services Terms Link. Customer must sign the Engagement Letter prior to any Project being performed. The signed Engagement Letter will become part of this SOW. In the event of a conflict between the terms and conditions of the Master Terms, the Professional Services Service Attachment (the "PSA"), this SOW, the SOF, and the Engagement Letter, the order of precedence shall be: the SOF, the PSA, the Master Terms, the SOW, and then the Engagement Letter.

1.2.4 **Cyber Incident Capability Assessments.** (Initial Assessment, as defined below, requires 0 Hours and subsequent Assessments use Hours as required)

1.2.4.1 An Engagement Letter is required for an Assessment.

1.2.4.2 The following cyber incident capability assessments are available. Customer may select one of these Assessments during each Onboarding session for zero Hours, (the "Initial Assessment"), with subsequent Assessments using Hours as required by the Assessment. The Engagement Letter will describe the specific scope and Deliverables for each of the Assessment options below.

- Incident Response Readiness Assessment;
- Network Health Checks;
- First Responders Training Course; or
- Executive Breach Simulation.

1.2.4.2.1 Incident Response Readiness Assessment. Verizon will review Customer's existing incident response capability, systems, platforms, data stores, and conduct a review of Customer's existing incident response policies and processes, tools, training, and testing initiatives to gain an understanding of the Customer's network infrastructure, electronic asset inventory, and threat profile. This Assessment may include:

- A review of Customer's existing incident response plan documentation, including written incident response policies and procedures;
- An interview of key incident response stakeholders to determine roles, responsibilities, and process within Customer's incident response plan;
- A review of relevant tools, platforms, technologies leveraged by Customer for incident response purposes; and
- Verizon will provide a report of recommendations and observations (the "Incident Response Assessment Report").

1.2.4.2.2 Network Health Checks. Verizon will capture and analyze 14 consecutive days of netflows stemming from Customer IP address ranges listed in the Customer IP ("CIP") schedule provided by Customer as requested by Verizon (the "CIP Schedule"). Verizon will analyze those traffic patterns matching Customer's identified CIP addresses against the Verizon watchlist. The watchlist contains IP addresses deemed suspect by Verizon based on the collection and scrutiny of intelligence drawn from the Verizon global IP backbone, investigations, and other sources. Verizon will match watchlist IP addresses against Customer inbound and outbound traffic to identify possible indications of unwanted activity.

1.2.4.2.2.1 Verizon will examine the metadata (e.g., source and destination IP addresses, source and destination ports, packet count and bytes) in Customer's inbound and outbound communications to search for known threat actors, as well as traffic patterns that are considered malicious. Verizon will supplement the netflow health check by IP-heavy firewall logs

Customer has obtained through Customer's security event management tool and provided to Verizon for analysis.

1.2.4.2.2.2 Verizon will provide Customer with a report of findings and recommendations (the "Network Health Check Report"). The Network Health Check Report will provide a brief executive summary, as well as details on the presence of potentially malicious, unauthorized, or unwanted activity, if any. Verizon will also provide recommendations related to the findings. The Network Health Check Report will explain Customer's strengths and weaknesses, and identify areas that can be improved.

1.2.4.2.3 First Responders Training Course. Verizon will provide training to Customer's first responders and/or members of Customer's incident response team ("Attendees"). Training focuses on basic skills and industry practices for first responders. Training modules includes topics such as proper evidence handling and chain of custody issues, collecting and preserving data of evidentiary value, including volatile data and forensic imaging techniques, and basic forensic analysis techniques.

1.2.4.2.3.1 Verizon will provide up to two (2) instructors to perform one (1) training course which will take place in two (2) days (maximum of sixteen (16) hours onsite) for up to twenty (20) Attendees. Topics included in the 2-day First Responder's training course include the following:

- Current security trends and incident response case studies;
- Incident response process;
- Evidence handling procedures;
- Volatile data collection and tactical analysis techniques;
- Forensic imaging techniques;
- Basic forensic analysis techniques – system analysis; and
- Mock incident table-top exercise.

1.2.4.2.3.2 Additional training topics may be offered on a case by case basis as shown in the Engagement Letter. The training course will be conducted during Verizon's normal business hours at a Customer Site and on a date mutually agreed to and detailed in the Engagement Letter.

1.2.4.2.3.3 Verizon will provide training materials ("Training Materials") and a certificate of training to Attendees.

1.2.4.2.4 Executive Breach Simulation. Verizon will conduct an executive breach simulation (the "Simulation") as a mock incident response exercise for Customer's senior executives. The objective of the Simulation is to evaluate Customer's existing processes and procedures for responding in real time to a computer security emergency.

1.2.4.2.4.1 The Simulation will be based on a mock security emergency scenario agreed by Verizon and Customer in advance, but not known to Customer's Simulation participants (the "Scenario"). Verizon will moderate the Simulation by introducing the Scenario and prompting Customer participants for feedback and participation relative to their respective areas of organizational responsibility. Verizon will then lead the Customer participants through the Scenario.

1.2.4.2.4.2 In advance of the Simulation, Verizon will work with a maximum of two Customer personnel ("Trusted Agents") to define the Scenario and the objectives, stages and duration of the Simulation. Subject to mutual agreement, the Scenario may address Customer's potential cyber security issues, which may include elements of a wide variety of cyber security incidents, including unauthorized access, malicious code, inappropriate use or abuse, phishing and social engineering, theft of sensitive data, and point-of-sale device compromise.

1.2.4.2.4.3 This service will be delivered during one (1) business day, and run for up to a four (4) hour period. Upon completion of the Simulation, Verizon will provide a report of observations and recommendations. (the "Executive Breach Simulation Report").

1.2.5 **Hotline Access.** (Requires 0 Hours)

Verizon will provide a toll-free support number to Customer that is available 24x7x365 (the "Hotline"). The Hotline is to be used by Customer when Customer has a security incident. Upon calling the Hotline, a Verizon representative will log the Customer's information and reason for the call, and will engage Investigative Team Phone Support as described below.

1.2.6 **Investigative Liaison.** (Requires 0 Hours)

Verizon will provide an investigative liaison ("Liaison") who will provide Customer with a consistent interface to Verizon's investigative team. The Liaison will serve as an alternate contact point to the Hotline, and in most cases will directly contribute to the delivery of Professional Services for Customer's reactive emergency response and proactive incident response consulting engagements.

1.2.7 **Investigative Team Phone Support.** (Uses Hours as required)

When Customer calls the Hotline with a suspected security incident, a member of Verizon's investigative team returns the Customer's call within the three-hour SLA to get more information related to the security incident. If the call requires a Project to be initiated, the investigative team member defines the scope of the Project in an Engagement Letter and schedules the Project for delivery as required.

1.2.8 **Emergency Services.** (Uses Hours as required)

1.2.8.1 An Engagement Letter is required for Emergency Services.

1.2.8.2 **On Site Response with In-Transit SLA.** When the Parties agree that a member of Verizon's investigative team must travel to a Customer Site, the Verizon investigative team member will be "in-transit" to the Customer Site within forty eight (48) hours of (a) Customer's execution of the Engagement Letter and (b) Verizon's procurement of all required travel documentation and Customer's approval if required. "In-transit" means the investigative team member is traveling to the Customer Site. The in-transit SLA clock begins when (a) and (b) are both complete and stops when the investigative team member is in-transit. Verizon's investigative team phone support is available while the investigative team member is in-transit.

1.2.8.3 **Emergency Services Phases.** Customer and Verizon will determine which of the following phases are required for an Emergency Services Project:

1.2.8.3.1 Incident Response Phase. The goal of the incident response phase is to contain and investigate an incident as necessary to bring the affected systems back into a trusted state. A key element in the incident response phase involves data collection by Customer or Verizon in the immediate aftermath of an incident. This phase can take place either onsite or remote, depending on the nature of the incident. Verizon will work with the Customer and will determine the appropriate response given the specific incident information provided by Customer, including:

1.2.8.3.1.1 Notification: Verizon will identify and alert the appropriate Verizon and Customer personnel of the incident so that a proper response can be formulated;

1.2.8.3.1.2 Assessment: Verizon will define the scope of the incident and identify data sources relevant to the incident. Data may be collected to help assess the severity of the incident and the necessary or recommended response. Collection and analysis of this data provides information to help Customer make a business decision on how to proceed with the incident response process.

1.2.8.3.1.3 Response and Acquisition: Verizon will respond based on the decisions made by Customer and Verizon during the assessment. A response may

include acquiring data from the affected system(s) for in-depth forensic analysis or increasing network monitoring to gather additional data. During response and acquisition, depending the nature and severity of the incident, Verizon may collect and preserve data of evidentiary value, establish a chain of custody for the data, and securely transport such data to a Verizon's forensic lab for further analysis.

1.2.8.3.1.4 Verizon Responsibilities. Verizon's response may include the following elements, depending on the nature of the incident:

1.2.8.3.1.4.1 Analysis: Verizon's analysis of relevant data to determine the source of the incident, its cause (program error, human error, or deliberate action), and its effects;

1.2.8.3.1.4.2 Containment: Verizon will work with Customer to prevent further data loss, and the effects of the incident from spreading to other computer systems and computer networks in the Customer's environment; and

1.2.8.3.1.4.3 Eradication: Verizon will work with Customer to remove instances of identified malware, or unprotected sensitive data so that the affected systems can be properly secured and brought back online by the Customer.

1.2.8.3.1.4.4 Report: Depending upon the nature of the engagement and Customer's request or if otherwise required, upon completion of the incident response phase, Verizon will produce a statement of preliminary findings (the "Preliminary Finding Report").

1.2.8.3.2 Forensic Analysis Phase. During the forensic analysis phase, Verizon will perform a further in-depth analysis on the data that was acquired during the incident response phase as well as gathering additional data for analysis. The objective of the forensic analysis is to reveal the source of the incident, method of intrusion, the extent to which sensitive data has been compromised, and any other details relevant to the investigation. This phase can take place either onsite or remote. Verizon will use analysis tools, knowledge of operating systems and file systems, and knowledge of vulnerabilities to identify evidence that can be used to determine the origin and details of the incident in accordance of the scope and objectives as stated in the Engagement Letter.

1.2.8.3.2.1.1 Methodology. Verizon will perform an analysis of the data to extract evidence. This analysis will be performed using a combination of open source, commercially available, and Verizon proprietary tools. During the analysis, Verizon will use several techniques to identify data including but not limited to:

- Analysis of allocated and unallocated files and directories;
- Timeline of file, application, and network activity;
- Analysis of unallocated file system space;
- Analysis of binaries to identify malicious code, determine its source and capabilities; and
- Analysis of file system structures to find evidence of anti-forensics activities.

1.2.8.3.2.1.2 Forensic Report. At the conclusion of the forensic analysis phase, Verizon will provide Customer with a management report ("Forensic Report") containing the specific findings of the investigation.

1.2.9 **Malcode Analysis.** (Uses Hours as Required)

1.2.9.1 An Engagement Letter is required for malcode analysis.

1.2.9.2 Malcode analysis provides analysis of files that Customer suspects might be malicious. Malcode analysis is limited as described herein and does not replace an Emergency Services forensic analysis. All files uploaded for malcode analysis must be isolated as individual files and may not be uploaded as part of a memory dump or network capture. Verizon will analyze no more than one file per 24-hour period.

1.2.9.3 Customer will upload malicious or suspicious files to the Verizon server for analysis. Instructions on how to upload files to the Verizon server will be provided to the Customer during the Onboarding session.

1.2.9.4 **Analysis.** Malcode analysis will typically focus on the interactions of the malcode with Customer's system. Verizon will attempt to determine the functionalities of suspected malicious files. Depending on the nature of the suspected malware functionality, the analysis may include identification of communication channels, a listing of indicators of compromise, and malware response guidelines. Malcode analysis may include the following, as determined by Verizon:

1.2.9.4.1 Code anatomy, which provides an overview of the malware binary content;

1.2.9.4.2 Behavioral analysis, which is a high level overview of the malcode's functioning with the objective of assisting in identifying system changes caused by the malcode and/or communication channels (e.g., IP addresses and domain names) utilized by the malcode; and

1.2.9.4.3 Malware intelligence analysis, which leverages Verizon's intelligence datasets to determine if the malware is already known and/or affiliated with known incidents or actors.

1.2.9.5 **Report.** Verizon will issue a report at the end of the analysis of the submitted code sample ("Malcode Analysis Report"), which will contain any identified findings, indicators of compromise and recommendations for additional analysis.

1.2.9.6 **Malcode Analysis SLA.** Verizon will perform an analysis of Customer's suspect files and provide Customer with the Malcode Analysis Report in a commercially reasonable timeframe. If additional analysis is required after the Malcode Analysis Report is issued, Verizon will continue with the service as described in the Engagement Letter.

1.2.10 **Verizon RISK Intelligence.** (Requires 0 Hours)

Verizon will email the Customer personnel identified at the Onboarding meeting with Verizon's research, investigations, solutions, and knowledge ("RISK") intelligence, which may include communications, such as weekly RISK intelligence summaries ("INTSUM"), monthly RISK intelligence briefings (phone and web conference), and other ad-hoc intelligence reports produced by Verizon's RISK intelligence team and/or compiled by other intelligence sources for distribution to Verizon's customers. Collectively, the INTSUM, monthly briefings, and ad-hoc intelligence reports are referred to herein as "Intelligence Reports."

1.2.11 **Project Management.** (Requires 0 Hours)

Verizon will be responsible for managing the change control process. Should the Project's requirements change during the course of a Project, Verizon will ensure that any modifications to scope, budgeted number of hours and schedule are appropriately documented in an amended Engagement Letter.

1.2.12 **Service Level Agreement ("SLA") Terms.**

1.2.12.1 The Professional Services listed below have SLAs as stated above. If Verizon fails to meet the respective SLA, Customer's sole and exclusive remedy shall be a credit of an additional five (5) Hours of security consulting support, which may be used within a Contract Year. For any Project described in an Engagement Letter, Customer's SLA remedy will be limited to five (5) Hours and must be used within a Contract Year. An SLA remedy will be documented in an Engagement Letter showing the increase in the security consulting support Hours at no additional cost to the Customer. The SLAs are described above for the following Professional Services:

- Investigative Team Phone Support;
- Emergency Services In-Transit SLA; and
- Malcode Analysis.

1.2.12.2 **SLA Conditions.**

1.2.12.2.1 No SLA remedy will be due to the extent the SLA is not met because of any act or omission on the part of the Customer, its contractors or vendors, or any other entity over which the Customer exercises control or has the right to exercise control.

1.2.12.2.2 No SLA remedy will be due to the extent the SLA is not met because of a Force Majeure event, as defined in the Agreement.

1.2.12.2.3 No SLA remedy will be due to the extent the SLA is not met because of the amount of time delays caused by incorrect or incomplete information provided by Customer.

2. **Deliverables and Documentation to be Produced by Verizon.** Deliverables are intended for Customer and Verizon use only. Customer may disclose a Deliverable to a third party pursuant to the Agreement's confidentiality terms.
   2.1. Deliverables provided as part of the Onboarding meeting will be in an escalation document that includes: i) the hotline number, ii) contact information for the Liaison, and iii) the Project initiation process with a sample Engagement Letter. Verizon will provide the server access process.
   2.2. Verizon will provide the following Deliverables as required for Professional Services ordered pursuant to an Engagement Letter for a Project:

      2.2.1. Deliverables as described in the individual Engagement Letters
      2.2.2. Network Health Check Report
      2.2.3. Training Materials
      2.2.4. Executive Breach Simulation Report
      2.2.5. Incident Response Assessment Report
      2.2.6. Preliminary Finding Report
      2.2.7. Forensic Report
      2.2.8. Malcode Analysis Report
      2.2.9. Intelligence Reports

3. **Documentation to be produced by Customer and Customer Obligations.** Delivery of Professional Services by Verizon is dependent on Customer's performance of the following:
   3.1. Customer agrees to provide the assistance as defined under Customer Obligation section of the Professional Services Service Attachment.
   3.2. For Professional Services requiring a CIP Schedule, Customer must provide a fully completed and executed CIP Schedule. Customer will go to the Professional Services Terms Link and download the CIP Schedule for completion and execution prior to commencement of a Project requiring a CIP Schedule and Verizon will confirm the IP addresses using public resources (e.g. ARIN, RIPE, APNIC, Google, etc.). Verizon will notify Customer of any IP address discrepancies and addresses which Verizon cannot confirm Customer's required ownership will not be collected.
      3.2.1. Customer represents and warrants that:
         3.2.1.1. the Deliverables, documentation, and other information provided by Verizon in connection with the Professional Services requiring a CIP Schedule will be used solely for purposes of protecting Customer from abusive, fraudulent, or unlawful use of Verizon's public Internet service;
         3.2.1.2. the list of Internet IP addresses provided by the Customer contains only IP addresses that have been assigned or allocated for the exclusive use of Customer and/or affiliates of Customer over which Customer has control; and
         3.2.1.3. it has obtained or will obtain all legally required consents and permissions from users of CIP for Verizon's performance of the Professional Services, including without limitation the collection, use, processing, analyses and disclosure to Customer of Customer's Internet traffic data.

3.2.2. Customer shall indemnify Verizon and Verizon affiliates, and Verizon's associates, officers, directors, employees, agents and partners ("Verizon Indemnities") from and against all losses, damages, costs and expenses (including allocable costs of in-house counsel and other legal fees) associated with any claims, suits, judgments, settlements, investigations, fines, consent decrees, requests for information, or other dispute resolution, enforcement, regulatory or legal proceedings or actions of any kind, suffered or incurred directly or indirectly by Verizon Indemnities from or arising out of Customer's breach of any of the representations and warranties immediately above.

3.2.3. Customer acknowledges that the Deliverables, documentation, security analyses and insight, and other information provided by Verizon in connection with Professional Services requiring a CIP Schedule ("Net Intel Information") are highly sensitive and that the obligations in this provision supplement and do not conflict with other terms in its Agreement. Customer will disclose Net Intel Information only to Customer employees with a "need to know" for purposes set forth in the Customer representations and warranties above and who are bound to confidentiality obligations at least as restrictive as those set forth in the Agreement. In no event may Customer use lesser efforts to protect Net Intel Information from use or disclosure not permitted under the Agreement than it uses to protect its own highly-sensitive confidential information, or less than reasonable efforts.

3.3. Customer will provide site authorization documentation as required.

3.4. Customer will designate a POC who will be responsible and authorized to (i) make all decisions and give all approvals which Verizon may need from Customer, and (ii) provide Verizon's personnel on a timely basis with all information, data and support reasonably required for its performance under this SOW, including but not limited to making available appropriate personnel to work with Verizon as Verizon may reasonably request.

3.5. Customer will provide Verizon all necessary approvals in a timely manner.

3.6. Customer will provide Verizon with copies of all configuration information, log files, intrusion detection events, and other forensic data relevant to the Incident and its analysis, as required.

3.7. Customer will manage the collection and dissemination of all information regarding an incident with Customer technical and managerial personnel, Customer legal and public relations departments, other organizations within Customer's enterprise, and other companies or business partners, as required.

3.8. Customer is responsible for the decision to implement (or not to implement) any recommendations and the results achieved from such implementation.

3.9. Customer is responsible for the implementation of any changes under this SOW to applications or devices managed by Customer or Customer's service providers.

3.10. Customer is responsible for the actual content of any data file, selection, and implementation of controls on its access and use, and security of stored data.

3.11. Unless otherwise required (e.g., by Payment Card Industry requirements), Customer is responsible for all notifications to outside parties, including law enforcement, of the results of the Professional Services.

4. **Assumptions.** Delivery of the Professional Services by Verizon is predicated on the following assumptions and conditions:

4.1. Customer retains responsibility for any coordination of the Professional Services to be performed at a business partner location.

4.2. Customer retains responsibility for travel expenses as provided in the Professional Services Service Attachment and the SOF.

4.3. Verizon and Customer must complete the Onboarding process before Customer orders Professional Services.

4.4. Notwithstanding the PSA, hours in which Emergency Services will be provided will be agreed by the Parties at the time the Emergency Service is performed.

4.5. **Permitted Use.** If a Professional Service involves data that is subject to the Payment Card Industry ("PCI") Security Standards Council (the "PCI Council") requirements on Customer, Verizon shall have the right to disclose the results of the Professional Services (including any report of compliance, working papers, notes and other information) to the PCI Council and other parties as required under the PCI Forensic Investigator ("PFI") Program Guide and the qualified security assessor ("QSA") Validation Requirements (Supplement for PCI Forensic Investigators) promulgated by the PCI Council. Copies of the PCI Council's current standard PCI Forensic Investigator Program Guide and QSA Validation Requirements (Supplement for PCI Forensic Investigators) are available on the PCI Council's website (see www.pcisecuritystandards.org).

5. **Project Delivery Countries.** Verizon will only deliver a Project within Customer Sites in the countries indicated by Customer in the Country List provided by Customer during initial Onboarding. Customer modifications to the countries selected in the Country List must be done pursuant to the Professional Services Service Attachment change order process. Notwithstanding the Country List, Verizon reserves the right to decline a Customer request to provide Professional Services at any Customer Site if, in Verizon's sole discretion: 1) the location or country is unsafe for Verizon personnel; 2) applicable tax, regulatory laws, rules, or regulations render performance of Professional Services in a location unreasonable, impracticable, or impossible; or 3) Verizon is unable to obtain a visa, entry permit, or similar authorization, where required.

5.1. **Projects Delivered in India.** Specifically as it relates to requests by Customer for Professional Services for locations in India, the following shall apply:

5.1.1. Professional Services performed for Customer locations in India shall be ordered separately with Verizon Communications India Private Limited. All security consulting support Hours incurred in India shall be invoiced by Verizon Communications India Private Limited directly to the Customer, pursuant to the terms of a Rapid Response Retainer India Service Order Form, the form of which can be found at the Professional Services Terms Link.

5.1.2. Any Hours, or SLA Hours, included in this SOW, if any, will not be available for use in India.